Havells India

Password Management Policy

Version 1.0

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Havells India Password Management Policy
2.	Document Code	HPMP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Document Scope

This document shall be applicable to the all employees/third parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees of Havells India by uploading it on the intranet.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose

The purpose of this policy is to establish rules for creation, distribution, safeguarding, termination, and reclamation of the user authentication mechanisms. Access to user accounts is controlled by an authentication mechanism utilizing unique user IDs and passwords. These authentication mechanisms ensure controlled and restricted access to the information and information systems according to the business requirements.

1.1 Scope & Audience

This document applies to:

a) All Employees, including but not limited to contractors, service providers, voluntary agencies, partners.

b) All regions of Havells business.

c) All Havells controlled and operated business entities.

1.2 Responsibility

All Functional Heads shall be responsible for the implementation of the Password Management in their respective function. Partner/ Third Party serving Havells, shall be responsible for the implementation of the Password Management Policy.

1.3 Enforcement

All Employees must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the standard.

Non-compliance with this standard shall be dealt with in accordance with the approved management process.

a) Employees and third parties who breach this standard shall be subject to disciplinary action.

b) In the case of third parties, appropriate clauses incorporated in the contract / agreement for violations / non-compliances of policy shall be invoked as per the specified process.

Requests for deviations from this standard must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the Information Security Policy.

1.4 Authority

The Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

2. Policy

2.1 User Responsibility

a) User shall change the default password at first logon;

b) Passwords shall be at least twelve characters in length with complexity;

c) Users shall change their password regularly at least once every 60 days;

d) Users shall be careful when entering the password. User will be locked if 5 repeated invalid attempts are made. User ID shall get unlocked automatically after 15 minutes or by taking IT support immediately;

e) It's mandatory to accept disclaimer message displayed on the logon screen on laptop and desktops;

Windows Servers / PCs will be auto locked after 15 minutes of inactivity. For QRG Hospital users other than doctors, Medical i.e. Nursing station/ front office users, this auto locked timeout is 15 minutes and for QRG doctors, Medicare i.e. Nursing station/ front office users it's 30 minutes;

f) Users shall avoid the use of the following to create passwords:

i. Employee ID or Contractor ID;

ii. Name of the User or names of family members;

iii. Address or phone number;

iv. Birth date of self or family members;

v. Any other personal information;

vi. A combination of months, seasons or years;

g) Users shall be responsible for any security incident/ breach that occurs under their logon accounts and are responsible for keeping their passwords confidential;

h) Users shall ensure that passwords for accessing Havells IT Systems and any personal accounts are not same. (E.g. personal banking, personal email accounts, etc.);

i) Do not write passwords anywhere (e.g. paper, note pad, computer files, shared drives, mobile devices, personal emails etc.).;

j) User shall ensure not to share password in any circumstances including email, phone etc.;

k) If a User finds or suspects that his/her password has been compromised, he/ she shall change it immediately and report the same to the IT support;

l) Users shall contact IT support for account and password assistance;

m) IT Support shall ensure to share password via automated mail or SMS on registered mobile no. or email id.

2.2 Password Management

This section is applicable to passwords of regular Users, and privilege Users.

Appropriate technical specifications for password management, shall be implemented on the Information Systems and applications:

a) Passwords shall contain the following four (4) categories:
   i. Alphabetic upper case (A-Z)
   ii. Alphabetic lower case (a-z)
   iii. Numeric (0-9)
   iv. Special character (` ~ {} @ etc.)

b) Password history shall be maintained for last 5 passwords set;

c) No hardcoded or unchangeable passwords shall be defined in the Information System (including SNMP community strings);

d) Ensure passwords are not coded into login scripts, dial-in communications programs, browsers or any executable program or file, wherever possible;

e) Secure mechanisms shall be used to encrypt and secure the passwords;

f) Change/Reset password functionality should only work after User identity is verified by the Information System or an Information System Administrator or IT support team;

g) Passwords should not be visible on a screen, hardcopy printouts or any other output device

2.3 Super User Password

a) All privileged user passwords for Operating Systems, Databases, Applications, and Network Equipment like routers, switches etc., shall be sealed in an envelope and kept in a fire-proof safe or Secure Vault (PIM) or TACAS. This is necessary in case the password is forgotten or the related person has left the organization without surrendering the passwords;

b) These sealed envelopes or secure vault(PIM) shall be opened / accessed with the permission of the Information Security Head / CIO. The password will be changed immediately and kept in a new sealed envelope or secure vault(PIM)

c) Accounts with Password “never expires” shall be reviewed half-yearly.

2.4 Disabling default passwords

a) Wherever applicable, Vendor Supplied User-IDs/Passwords, encryption keys, and other access codes included with vendor-supplied systems shall be changed before a new system is brought on-line. Similarly, default passwords shipped with software shall be disabled or changed before the software is deployed in the production environment

2.5 Confidentiality of Password

a) All User (normal users, administrators) passwords shall remain confidential and not shared, posted or otherwise divulged in any manner;

b) Passwords shall be stored in an encrypted format and not in clear text on computer systems;

c) Passwords shall not be displayed on system reports.